Quantum Passwords

Christian Weedbrook[1] and Mile Gu[1]

[1]*Department of Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

(Dated: February 1, 2008)

A quantum password is a quantum mechanical analogue of the classical password. Our proposal is completely quantum mechanical in nature, i.e. at no point is information stored and manipulated classically. We show that, in contrast to quantum protocols that encode classical information, we are able to prevent the distribution of reusable passwords even when Alice actively cooperates with Eve. This allows us to confront and address security issues that are unavoidable in classical protocols.

I. INTRODUCTION

Alice, a physicist, decides to purchase a subscription to a well known online physics journal that is run by an entity we shall call Bob. Once the transaction is complete, she is given a password that allows her access to the journal, a password that can be distributed at will. In particular, Alice gives the password to her friend Eve, who then resells it to the horde of independent physicists interested only in obtaining the journal at a cheaper price. Even if Alice were only to distribute the password to three of her closest friends, Bob's income would be a quarter of what it should be. Yet, there is no guaranteed method in which Bob can prevent and detect such behavior.

In this new age of information, passwords have become an essential part of everyday life, used for e-mails, bank accounts, CD-keys and a multitude of online products. Yet such passwords are often saved on a customer's computer, easily vulnerable to viruses and trojan attacks. Once such information is extracted by Eve, she is free to mass distribute it, exacerbating everything from piracy, unlawful reselling to the more serious cases of identity theft. For example, CD-keys are often used as a method to prevent piracy, especially for programs that involve an online service. Yet, nothing prevents a person from purchasing the software and copying it, writing down the key and returning it under a standard money back guarantee.

Classically, the only proven method to prevent password sharing is the use of one-time passwords, where a different password is required each time Alice accesses the system. Such a protocol creates a number of inconveniences, such as the unsuitability for group licenses, where a service is sold to a specified number of people. Also, Eve can steal one-time passwords at no risk, as she does not disturb Alice or Bob's system until she uses the password.

Can the laws of quantum mechanics guarantee the security of Alice's information, even from herself? So that there always exists a test that Alice can make to determine if Eve has taken her password before Eve makes use of it. In this way Bob can be fully confident that the service he sells cannot be distributed or resold to multiple people. In this paper, we propose a quantum analogue of the classical password, whose security is guaranteed by the no-cloning theorem [1]. In contrast to the classical one-time password scheme, our quantum password is not one time. Also the fact that Eve can be detected as soon as she takes the password, discourages any attempt to do so.

While our proposal shares some similarities in aim with quantum identification schemes [2, 3] and quantum cryptography protocols [4], it has one critical distinction. We do not assume Alice's station is secure, or even that she is on Bob's side. In particular, all of the aforementioned protocols involve a password stored as classical information which is encoded into a quantum state for transmission. While they guarantee security during transmission, Alice's password, stored at her station, can always be cloned without detection. The only previous proposal [5] in this area was one time, and demonstrated to be equivalent to proposals based on classical correlations [6]. In this paper, we argue that a password can be verified using an entirely physical process, and unlike classical documents, need not be read by a human being. Therefore it is not necessary for a password to be an encoding of classical information.

We propose a quantum password represented entirely by a quantum state that has no set basis of measurement and encodes no classical information. Since our protocol does not require Alice to have any knowledge of this quantum state, the no-cloning theorem can be easily employed. Thus Alice cannot distribute her password to anyone, short of giving it away and consequently losing her only copy. Therefore there is only one quantum password existing, per person, at any one time. In addition, the quantum nature of the password means that it cannot be measured exactly, and allows our protocol to retain its security even when Bob's login server in vulnerable. That is, even if Eve has access to Bob's login server, she still cannot access the restricted content without detection. This is not possible classically and is a further distinction from the one-time password protocol.

II. QUANTUM PASSWORD PROTOCOL

The standard protocols of classical passwords can be divided into various stages: the creation of an account when Alice signs up for a service provided by Bob, the distribution of the password from Alice to Bob, and the process of password verification by Bob. More explicitly, Alice would purchase the password from Bob, which is used for verification each time she wishes to access Bob's product. In the quantum version of this protocol, all three steps are kept intact (see Fig. 1). The major difference is that the password itself will be a quantum object, and the process of transmission and verification are both done quantum mechanically.

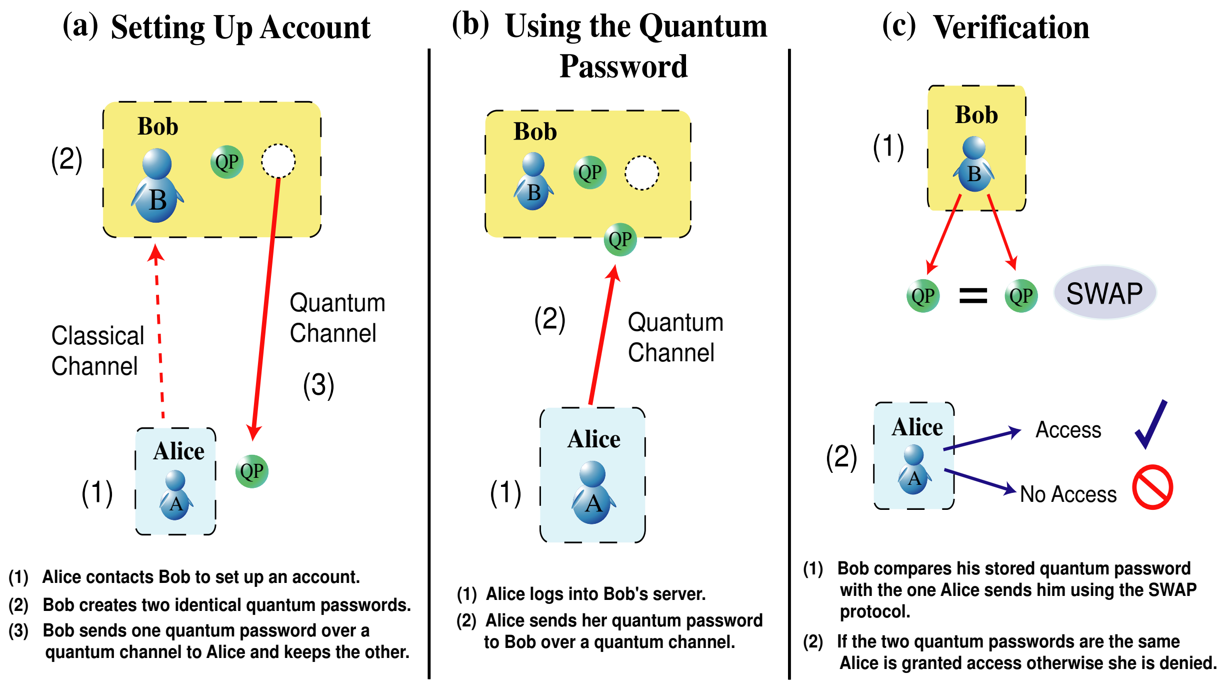
(a) Setting Up Account
Bob
(2)
B
QP
Classical Channel
Quantum Channel
(3)
Alice
(1)
A
QP
(1) Alice contacts Bob to set up an account.
(2) Bob creates two identical quantum passwords.
(3) Bob sends one quantum password over a quantum channel to Alice and keeps the other.
(b) Using the Quantum Password
Bob
B
QP
QP
(2)
Quantum Channel
Alice
(1)
A
(1) Alice logs into Bob's server.
(2) Alice sends her quantum password to Bob over a quantum channel.
(c) Verification
(1)
Bob
B
QP
=
QP
SWAP
(2)
Alice
A
Access
No Access
(1) Bob compares his stored quantum password with the one Alice sends him using the SWAP protocol.
(2) If the two quantum passwords are the same Alice is granted access otherwise she is denied.

FIG. 1: **The quantum password protocol can be broken up into three stages: (a) setting up the account (b) using the quantum password and (c) the verification by Bob. Here Alice's quantum password is given by ϕ and Bob's stored copy of the password given by ψ.**

A. Assumptions

Since the passwords featured within this protocol are not encodings of classical information, we are able to make several significant relaxations to the assumptions made in quantum cryptography [4]. As aforementioned, we assume that Alice's server is insecure, and in addition, Eve also has the ability to extract information from Bob's log-in server. These conditions are realistic, given that it is no harder, and often easier to install viruses into another's computer than to extract information during transmission.

However we do assume that there exists an unjammable classical public channel between Alice and Bob, such that Alice is able to contact Bob should her password be compromised. When these conditions are met, the protocol is completely secure, where security is defined by the fact that Eve cannot take the password without disturbing the system, and hence cannot escape detection. Explicitly, if Eve gains any information about the quantum password, there exists a finite probability that she will be detected.

B. Setting up the Quantum Password

Alice contacts Bob who organizes to give Alice her own quantum password (along with a classical username which will be omitted in further discussion). For simplicity, we consider that each password consists of only one qubit. In practice, the quantum password would consist of many qubits, so that the probability of a successful random guess is negligible. Bob generates a random password given by

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle \tag{1}$$

where $|c_1|^2 + |c_2|^2 = 1$, and creates an identical clone $|\phi\rangle$ - this does not violate the no-cloning theorem as the state is known to Bob. Bob stores his cloned qubit in quantum memory and sends the other qubit to Alice through an insecure quantum channel.

C. Using the Quantum Password

In order for Alice to use her quantum password, she sends it back along the quantum channel to Bob. Bob then needs to compare his stored copy of Alice's quantum password $|\phi\rangle$ with the quantum password Alice has sent to him $|\psi\rangle$. If both passwords are identical, then Bob will allow Alice access to his computer.

D. Verifying the Quantum Password

To compare the two quantum passwords $|\phi\rangle$ and $|\psi\rangle$, Bob performs a controlled-SWAP operation [7] using a Fredkin gate [8] to determine if they are identical (see Fig. 2). The advantage is that this operation can be performed without explicit knowledge of either of the quantum passwords. Explicitly, Bob introduces an ancilla qubit and performs the operation

$$|\gamma\rangle = (\hat{H} \otimes \hat{I})(\mathrm{c}-\mathrm{SWAP})(\hat{H} \otimes \hat{I})|0\rangle|\phi\rangle|\psi\rangle \tag{2}$$

where $\hat{H}$ is the Hadamard operator that transforms $|\mathrm{a}\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\mathrm{a}}|1\rangle)$ with $\mathrm{a} \in (0,1)$ and acts only on the Hilbert space of the ancilla qubit $|0\rangle$. $\hat{I}$ is the identity operator acting only on $|\phi\rangle|\psi\rangle$. The controlled-SWAP is the operation which swaps the states $|\phi\rangle$ and $|\psi\rangle$ depending on the parity of the ancilla qubit. That is, it performs the SWAP operation

$$|\phi\rangle|\psi\rangle \rightarrow |\psi\rangle|\phi\rangle \tag{3}$$

if the state of the ancilla qubit is $|0\rangle$ and acts as the identity if the qubit is $|1\rangle$. The resulting state of the system can be written as

$$|\gamma\rangle = \frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle) + \frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle - |\psi\rangle|\phi\rangle). \tag{4}$$

Bob will now measure the ancilla qubit in the computational basis $|0\rangle$ and $|1\rangle$ with outcome probabilities given by

$$P(1) = |\langle 1|\gamma\rangle|^2 = \frac{1}{2}(1 - |\langle\phi|\psi\rangle|^2), \tag{5}$$

$$P(0) = |\langle 0|\gamma\rangle|^2 = \frac{1}{2}(1 + |\langle\phi|\psi\rangle|^2), \tag{6}$$

If the two quantum passwords are identical, i.e. $|\phi\rangle = |\psi\rangle$, then from Eqs. (5,6) we have $P(1) = 0$ and $P(0) = 1$. Thus if Bob were to measure 1, he knows with certainty that the supplied password is incorrect. However if he were to measure 0, he would assume the password to be correct and allow access. Note that since $P(0) < 1$ when the states are not identical, extending the length of the quantum password will ensure that Eve cannot achieve success through a random guess. Additionally, should the passwords be identical, this measurement process will leave the quantum passwords unchanged. Therefore the quantum password is reusable and not a one-time password equivalent.

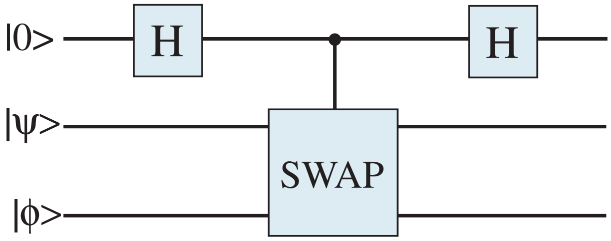

FIG. 2: **Schematic of the quantum circuit used by Bob to verify Alice's quantum password; where H is a Hadamard gate and the controlled-SWAP is achieved using a Fredkin gate.**

III. SECURITY OF QUANTUM PASSWORDS

The security of the quantum password scheme is due to the no-cloning theorem [1] which states that an unknown quantum state cannot be perfectly cloned. In addition, any measurement made on such a state will in general disturb it. In order for Eve to steal Alice's password without any chance of detection, she would be required to take it from Alice's station or intercept it during transmission, clone it perfectly and then return the original password without detection. Since we assume Alice's station is not secure, Eve is free to perform the first and final steps, but can only perform an approximation of the second.

Suppose Eve were to make an attempt in breaching the security of the quantum password protocol. That is, she desires to create a quantum state $|\phi'\rangle$ that is a good approximation to the true password $|\phi\rangle$ without detection from Alice or Bob. Eve is forbidden to modify Alice's password significantly, since doing so would cause Alice's password to fail during the SWAP verification and hence reveal her actions. Let us first assume Eve uses the symmetric universal quantum cloning machine [9]. Given an input state $|\phi\rangle$, the cloning machine would output two identical cloned quantum passwords with a fidelity of $5/6$ with respect to the original input. For qubit states, the two clones can be described by the same density operator

$$\hat{\rho}_{out} = \frac{5}{6}|\phi\rangle\langle\phi| + \frac{1}{6}|\psi\rangle\langle\psi| \tag{7}$$

where $|\psi\rangle$ is a quantum state containing the errors of the cloning machine and is orthogonal to $|\phi\rangle$, i.e. $\langle\psi|\phi\rangle = 0$.

In order for Eve to steal the password successfully, two events must occur. Firstly, Alice's quantum password must not be disturbed to the point where she can no longer access Bob's network, and secondly, the clone she has created must be accepted by Bob's server. Clearly, for a quantum password consisting of a single qubit, Eve chance of successfully using a clone is given by $(5/6)^2 \approx 69\%$ (see Fig. 3). Thus, for a quantum password of N qubits in length, Eve's success rate is reduced exponentially to $(5/6)^{2N}$.

In the more general case where Eve utilizes two nonidentical clones from an asymmetrical quantum cloning machine [10], it can be demonstrated that the fidelity of the clone F_S, and the password after measurement with respect to the original input F'_S, must satisfy the relation $F_S F'_S \leq 5/6$ [11]. Thus Eve's success rate is always bounded by $(5/6)^{2N}$. Therefore, provided we use a quantum password of sufficient length, the security of the protocol is guaranteed against such an attack.

Additionally, by assuming that Bob's login server is also insecure, Eve has the option of cloning Bob's quantum password instead. However, since Bob has knowledge of what the password is, he can always check whether it has been modified by comparing it to an offline (and thus secure) copy of the password. Should such a comparison fail at any time, he would generate a new quantum password and eliminate any information Eve may have gained from the state. Thus, the analysis of security for such an attack is reduced to the previous case.

IV. APPLICATIONS OF QUANTUM PASSWORDS

Passwords were designed with the intention of providing secure services, in the sense that such services can only be

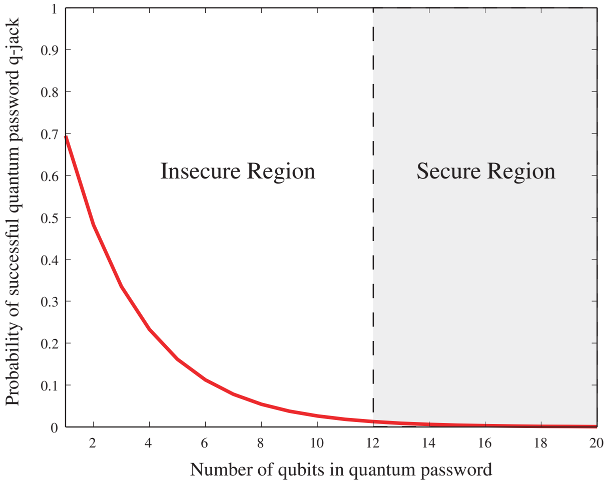

FIG. 3: **Probability that Eve can successfully use a clone of a quantum password verses the number of qubits contained in the password. Eve's success rate is bounded by $(5/6)^{2N}$ due to the fidelity of her quantum cloning machine. If Bob uses 13 or more qubits, then he is guaranteed that a fraudulent password will be detected at least 99.9% of the time.**

used by authorized parties. The ability to clone and distribute a password clearly violates this intention, and, is greatly detrimental to any service which involves the use of such devices. As quantum passwords cannot be cloned, it is potentially applicable to any protocol that involves a variation of the classical password. For example:

1. CD-keys are currently a widely used method to prevent piracy, used to validate the authenticity of a program whenever a user attempts to access some related online service. Suppose Alice runs a cybercafe with such programs installed. CD-key grabbers are commonly available for a visitor, Eve, to steal the key. If the passwords were made quantum, any such attempts can by easily detected by quantum password verification prior to Eve's departure from the cybercafe. Therefore, the chance of being caught on the spot will severely discourage such attempts.

2. Credit Card numbers are a variation of classical passwords. If Alice were to purchase concert tickets over the phone, she would need to give the information required to access her account to a third party operator, effectively cloning her password. The operator, can now retain and distribute this knowledge at her leisure. This problem cannot be circumvented using either classical or quantum cryptography since the operator, by definition, must have all the necessary knowledge to access Alice's account. A quantum password prevents this problem, as the operator must return the password back to Alice, and any attempt to extract information during the process could be detected.

3. Variations of the quantum password protocol can be implemented for ATM transactions where we need not assume security of either the client Alice, or even the login server, i.e. the ATM itself. Alice's quantum bank card stores a quantum state, which is matched by a clone on the bank's central server. Upon a transaction request, Bob sends his quantum password to the appropriate ATM and performs the verification protocol. Even if Eve had access to the ATM, she would still be unable to use it without detection. Classical solutions, such as the S/Key one-time password scheme [12], based on the computational difficulty of inverting the cryptographic hash function, are not formally secure.

V. DISCUSSION

Quantum passwords adopt a purely quantum approach to password identification, and in doing so, provides security that no classical protocol, or quantum protocol that involves the encoding of classical information, can offer. The implementation of quantum passwords will require reliable quantum memory and quantum gates. However, there is no explicit need for universal quantum processors and is a protocol that can be achieved in the medium term.

In this paper, we have outlined the idea of quantum passwords in the simplest possible implementation using a string of qubits, though in reality, this need not be so. One can note that the verification process does not assume that the quantum password lives in any specific Hilbert space, and thus, one can envision encoding such passwords in higher dimensions. For example, a continuous variable version would be able to take advantage of the high detection efficiencies and higher information bandwidths.

Future work could also be done in the analysis of how information loss due to noise or decoherence would affect the security of the protocol. In this case, Bob would need to take into account the natural losses during storage and transmission, and accept Alice's password provided a certain proportion of the qubits matched according to the SWAP protocol. Of course, this leeway would give a greater chance of using a cloned password, and one would be interested in the region where the protocol remains secure against such losses.

VI. CONCLUSION

In conclusion, we have introduced a quantum password scheme whose security is guaranteed by the no-cloning theorem. When implemented, such a protocol would allow consumers to purchase items over the phone without worry, knowing that they could check if the operators on the other end have copied down their credit card details. It would give subscription services the peace of mind that the passwords they sell cannot be distributed over the internet. It also bestows the added security when the login server itself becomes vulnerable, such as an ATM. Such security is made possible since our password is not a quantum encryption of classical information, but simply a quantum state. In short, we take advantage of the fact that passwords are meant to be used, not read.

We would like to thank Tim Ralph, Mark Dowling and Henry Haselgrove for comments and useful discussions.

[1] W.K. Wooters and W.H. Zurek, *Nature* **299**, 802 (1982).

[2] C. Crepeau and L. Salvail in *Advances in Cryptography: Proceedings of Eurocrypt '95* (Springer, Berlin, 1995), p. 133.

[3] H. Guang-Qiang and Z. Gui-Hua, *Chinese Physics*, **14**, 0541-05, (2005).

[4] C.H. Bennett and G.Brassard, in *Proceedings IEEE International Conference on Computers, Systems and Signal Proceedings (Bangalore)* (IEEE, New York, 1984), pp. 175-179.

[5] T. Mihara, Phys. Rev. A **65**, 052326, (2002).

[6] W. van Dam, Phys. Rev. A **68**, 026301 (2003).

[7] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, *Phys. Rev. Lett.* , **87**, 167902, (2001).

[8] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[9] V. Bužek and M.Hillery, Phys. Rev. A **54**, 1844 (1996).

[10] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998); V. Bužek *et al.*, Acta Phys. Slov. **48**, 177 (1998); N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998); N. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).

[11] R. Filip, Phys. Rev. A **69**, 032309 (2004).

[12] L. Lamport, Communications of the ACM, 770-772, (1981).